CLAIMS:

1. A method for performing on behalf of a registered user an operation on data stored on a publicly accessible data access server coupled to a client machine used by the registered user in such a manner as to prevent unauthorized users from using said data and without requiring decryption by the client machine, said registered user having a unique identifier known to the data access server and further having a password accessible to the data access server, said unique identifier being saved in the data access server in a user space associated with the registered user, said registered user further having a public key and a private key that is encrypted with said password to generate an encrypted private key that is stored together with the public key in said user space, the method comprising the following steps all carried out by the data access server:

(a) receiving from a user a login request including an identifier of said user and supplementary data that may be used to authenticate the user,

(b) verifying that the user is a registered user,

(c) if the user is a registered user:

i) receiving a request by the registered user for performing said operation together with a session ID of said user that is allocated to the user during login and is known to the login server,

ii) communicating the session ID of said user to the login server for identification thereby,

iii) receiving from the login server the user's password encrypted in such a manner as to enable decryption by the data access server,

iv) decrypting the encrypted password so as to derive the password associated with the user during the login request,

v) attempting to decrypt the encrypted private key of the registered user having said unique identifier using said password, and

vi) if the registered user's private key is successfully decrypted, using the registered user's private key to perform said operation on behalf of the registered user.

2. The method according Claim 1, wherein the supplementary data serves as said password.

3. The method according Claim 2, wherein during login the data access server further performs the following steps:

(1) encrypting the password so as to generate an encrypted password, and

(2) sending the encrypted password to a login server coupled to the data access server for storage thereby;

whereby the data access server may access the password from the login server without storing it locally.

4. The method according to Claim 3, wherein in step **(2)** the encrypted password sent to the login server is adapted for temporary storage thereby during a current session only.

5. The method according to Claim 4, further including:

vii) informing the login server upon termination of the current session so as to allow deletion of the encrypted password thereby.

6. The method according Claim 1, wherein during login the data access server further performs the following steps:

(1) using the supplementary data to generate said password.

7. The method according Claim 6, wherein during login the data access server further performs the following steps:

(2) encrypting the password so as to generate an encrypted password, and

(3) sending the encrypted password to a login server coupled to the data access server for storage thereby;

whereby the data access server may access the password from the login server without storing it locally.

8. The method according Claim 1, wherein the password is previously known to the login server and step **(c)iii)** includes:

(1) sending the unique identity of the user to the login server, and

(2) receiving the password from the login server;

whereby the data access server may access the password from the login server without storing it locally.

9. The method according to Claim 1, wherein in steps **(c) iii)** and **iv)** the password associated with the user is encrypted with a public key of the login server so as to enable decryption by the data access server using its public key and subsequent decryption using private key.

10. The method according to Claim 2, wherein step **(b)** includes:

ii) generating a fingerprint of the password and comparing with a fingerprint stored in the user space associated with the registered user identified by said unique identifier.

11. A method for performing on behalf of an authorized user an operation on data stored on a publicly accessible data access server coupled to a client machine used by the registered user in such a manner as to prevent unauthorized users from using said data and without requiring decryption by the client machine, said user having a unique identifier known to the data access server and further having a password accessible to the data access server, said unique identifier being saved in the data access server in a user space associated with the registered user, said authorized user further having a public key and a private key that is encrypted with said password to generate an encrypted private key that is stored together with the public key in said user space, the method comprising the following steps all carried out by a login server coupled to the data access server:

(a) receiving from the data access server a session ID of said user associated with a current session that is allocated to the user during login and is known to the login server,

(b) using the session ID of said user to retrieve the user's password, and

(c) sending to the data access server the user's password encrypted in such a manner as to enable the data access server to:

i) decrypt the encrypted password so as to derive the password associated with the user during a login request,

ii) attempt to decrypt the encrypted private key of the registered user having said unique identifier using said password, and

iii) if the registered user's private key is successfully decrypted, using the registered user's private key to perform said operation on behalf of the registered user.

12. The method according to Claim 11, further including:

(d) receiving from the data access server notification upon termination of the current session, and

(e) deleting the encrypted password.

13. The method according to Claim 12, further including:

(f) automatically logging out the user after a predetermined timeout period, and

(g) deleting the encrypted password.

14. The method according to Claim 11, further including during logon by the user to the data access server:

(h) receiving from the data access server an encrypted password of the registered user, and

(i) storing the encrypted password in a user space of the login server associated with the registered user for subsequent access by the data access server.

15. The method according to Claim 11, wherein said password is provided during logon by the user to the data access server.

16. The method according to Claim 11, further including:

viii) decrypting the user's encrypted password using the login server's private key and re-encrypting using a temporary key that is stored only in random access memory, and

ix) saving the re-encrypted password.

17. The method according to Claim 16, wherein the temporary key is a symmetric key.

18. The method according to Claim 16, wherein the temporary key is generated periodically.

19. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for performing on behalf of a registered user an operation on data stored on a publicly accessible data access server coupled to a client machine used by the registered user in such a manner as to prevent unauthorized users from using said data and without requiring decryption by the client machine, said registered user having a unique identifier known to the data access server and further having a password accessible to the data access server, said unique identifier being saved in the data access server in a user space associated with the registered user, said registered user further having a public key and a private key that is encrypted with said password to generate an encrypted private key that is stored together with the public key in said user space, the method comprising the following steps:

(a) receiving from a user a login request including an identifier of said user and supplementary data that may used to authenticate the user,

(b) verifying that the user is a registered user,

(c) if the user is a registered user:

i) receiving a request by the registered user for performing said operation together with a session ID of said user that is allocated to the user during login and is known to the login server,

ii) communicating the session ID of said user to the login server for identification thereby,

iii) receiving from the login server the user's password encrypted in such a manner as to enable decryption by the data access server,

iv) decrypting the encrypted password so as to derive the password associated with the user during the login request,

v) attempting to decrypt the encrypted private key of the registered user having said unique identifier using said password, and

vi) if the registered user's private key is successfully decrypted, using the registered user's private key to perform said operation on behalf of the registered user.

20. A computer program product comprising a computer useable medium having computer readable program code embodied therein for performing on behalf of a registered user an operation on data stored on a publicly accessible data access server coupled to a client machine used by the registered user in such a manner as to prevent unauthorized users from using said data and without requiring decryption by the client machine, said registered user having a unique identifier known to the data access server and further having a password accessible to the data access server, said unique identifier being saved in the data access server in a user space associated with the registered user, said registered user further having a public key and a private key that is encrypted with said password to generate an encrypted private key that is stored together with the public key in said user space, the computer program product comprising:

computer readable program code for causing the computer to receive from a user a login request including an identifier of said user and supplementary data that may used to authenticate the user,

computer readable program code for causing the computer to verify that the user is a registered user,

computer readable program code responsive to the user being a registered user for causing the computer to receive a request by the registered user for performing said operation together with a session ID of said user that is allocated to the user during login and is known to the login server,

computer readable program code responsive to the user being a registered user for causing the computer to communicate the session ID of said user to the login server for identification thereby,

computer readable program code responsive to the user being a registered user for causing the computer to receive from the login server the user's password encrypted in such a manner as to enable decryption by the data access server,

computer readable program code responsive to the user being a registered user for causing the computer to decrypt the encrypted password so as to derive the password associated with the user during the login request,

computer readable program code responsive to the user being a registered user for causing the computer to attempt to decrypt the encrypted private key of the registered user having said unique identifier using said password, and

computer readable program code responsive to the user being a registered user and to the registered user's private key being successfully decrypted for causing the computer to use the registered user's private key to perform said operation on behalf of the registered user.

21. A data access server for effecting a secure transaction on behalf of a user accessing the data access server via a client machine, the data access server comprising:

a first communication port for coupling the client machine thereto,

a second communication port for coupling a login server thereto,

a processor coupled to the first communication port and to the second communication port,

a memory coupled to the processor storing a user identity in respect of a registered user and a private key encrypted with a password of said user,

a receive unit coupled to the processor for receiving from a user a login request including an identifier of said user and supplementary data that may be used to authenticate the user,

a verification unit coupled to the receive unit for verifying that a user is registered,

a command unit coupled to the processor for receiving a request by the registered user for performing a desired operation together with a session ID of said user that is allocated to the user during login and is known to the login server,

a password retrieval unit coupled to the second communication port for communicating the session ID of the user to the login server for identification thereby and for receiving from the login server the user's password encrypted in such a manner as to enable decryption by the data access server,

a first decryption unit coupled to the password retrieval unit for decrypting the encrypted password so as to derive the password associated with the user during a login request, and

a second decryption unit for decrypting the encrypted private key of the registered user having said unique identifier using said password.

22. The data access server according to Claim 21, further comprising a third communication port for coupling thereto a backup repository allowing retrieval of the user's password.

23. A login server comprising:

a communication port for coupling a data access server thereto,

a processor coupled to the communication port,

a memory coupled to the processor storing a user identity in respect of a registered user and an encrypted password of said user,

a login request unit coupled to the processor for receiving from the data access server a login request including an identifier of said user,

a session ID allocation unit coupled to the login request unit for allocating a session ID relating to a current connection session with the data access server and storing the session ID in said memory in association with the user identity of said user,

a password retrieval unit coupled to the communication port for receiving the session ID from the data access server and retrieving the encrypted password of the user,

a decryption unit coupled to the password retrieval unit for decrypting the encrypted password so as to derive the password associated with the user during a login request, and

an encryption unit coupled to the decryption unit for encrypting the private key of the registered user in such a manner as to enable decryption by the data access server.